

CLAIMS

I claim:

1. A system for archiving data blocks comprising:
a user data processing means for a user to form one or more data blocks;
transmission means, coupled to the user data processing means, for transmitting said data blocks from the user data processing means; and
remote archive storage means, coupled to the transmission means, for receiving and storing the one or more data blocks, said remote archive storage means preventing anyone, including the user, from modifying or deleting said one or more data blocks stored at said remote archive storage means to provide non-rescindable storage of said data blocks for at least an initial time period.
2. The system of claim 1, wherein the user negotiates the initial time period with the remote archive storage means to reach agreement on an initial time period for non-rescindable storage of said one or more data blocks.
3. The system of claim 1, further comprising:
means for retrieving, from the remote archive storage means to the user, a copy of the one or more data blocks.
4. The system of claim 1, further comprising:
digital signature generating means, coupled to said user data processing means, for computing for the user, a secure digital signature data block comprising a secure digital signature of

the one or more data blocks, and appending the digital signature data block to the one or more data blocks.

5. The system of claim 4, wherein the digital signature generating means comprises a digital signature generating party independent of the user data processing means, and coupled to the user data processing means via the transmission means.

6. The system of claim 1, further comprising:
secure time-stamping means coupled to the user data processing means and the remote archive storage means for receiving the one or more data blocks and time-stamping the one or more data blocks on receipt, and storing said time-stamp as an additional non-rescindable data block with the one or more data blocks in the remote archive storage means.

7. The system of claim 6, wherein the secure time-stamping means comprises a secure time-stamping party, independent of the user data processing means and the remote archive storage means, coupled to the user data processing means and the remote archive storage means by the transmission means.

8. The system of claim 1, further comprising:
encryption means, coupled to the user data input means and the remote archive storage means, for encrypting the one or more data blocks to create one or more encrypted data blocks, and transmitting said one or more encrypted data blocks to remote archive storage means in place of said one or more data blocks.

9. The system of claim 8, wherein the encryption means comprises an encryption party, independent of the user data processing means and the remote archive storage means, coupled to the user data processing means and the remote archive storage means via the transmission means.

10. The system of claim 1, further comprising:

filing key generating means, coupled to said user data input means and said remote archive storage means, for generating filing keys from said one or more data blocks.

11. The system of claim 10, wherein said filing key generating means comprises an independent filing key generating party, independent of the user data processing means and the remote archive storage means, coupled to the user data processing means and the remote archive storage means via the transmission means.

12. The system of claim 1, further comprising:

search means to search stored filing keys at said remote archive storage means to select at least one of the one or more data blocks for retrieval of copies of the at least one of the one or more data blocks.

13. The system of claim 12, wherein said search means comprises an independent search party, independent of the user data processing means and the remote archive storage means, coupled to the user data processing means and the remote archive storage means via the transmission means.

14. The system of claim 1, further comprising:

encryption means for encrypting the one or more data blocks to produce one or more encrypted data blocks such that the remote archive storage means may not decrypt the one or more encrypted data blocks but that the user may decrypt copies of the one or more encrypted data blocks.

15. The system of claim 14, wherein said encryption means comprises an independent encryption party, independent of the user data processing means and the remote archive storage means, coupled to the user data processing means and the remote archive storage means via the transmission means.

16. The system of claim 1, further comprising:

voice waveform data input means, coupled to said user data processing means, for receiving a user's voice and creating voice waveform data; and

voice recognition and transcription means, coupled to said user data processing means and said remote archive storage means, for generating one or more text data blocks from said voice waveform data transmission for storage in the remote archive storage means.

17. The system of claim 16, wherein said voice recognition means comprises an independent voice recognition and transcription party, independent of the user data processing means and the remote archive storage means, coupled to the user data processing means and the remote archive storage means via the transmission means.

18. The system of claim 2, further comprising:

digital signature generating means, coupled to said user data processing means, for computing for the user, a secure digital signature data block comprising a secure digital signature of the one or more data blocks, and appending the digital signature data block to the one or more data blocks.

19. The system of claim 2, further comprising:

secure time-stamping means coupled to the user data processing means and the remote archive storage means for receiving the one or more data blocks and time-stamping the one or more data blocks on receipt, and storing said time-stamp as an additional non-rescindable data block with the one or more data blocks in the remote archive storage means.

20. The system of claim 18, further comprising:

secure time-stamping means coupled to the user data processing means and the remote archive storage means for receiving the one or more data blocks and time-stamping the one or more data blocks on receipt, and storing said time-stamp as an additional non-rescindable data block with the one or more data blocks in the remote archive storage means.

21. The system of claim 2, further comprising:

encryption means, coupled to the user data input means and the remote archive storage means, for encrypting the one or more data blocks to create one or more encrypted data blocks, and transmitting said one or more encrypted data blocks to remote archive storage means in place of said one or more data blocks.

22. The system of claim 20, further comprising:

encryption means, coupled to the user data input means and the remote archive storage means, for encrypting the one or more data blocks to create one or more encrypted data blocks, and transmitting said one or more encrypted data blocks to remote archive storage means in place of said one or more data blocks.

23. The system of claim 2, further comprising:

filing key generating means, coupled to said user data input means and said remote archive storage means, for generating filing keys from said one or more data blocks.

24. The system of claim 22, further comprising:

filing key generating means, coupled to said user data input means and said remote archive storage means, for generating filing keys from said one or more data blocks.

25. The system of claim 2, further comprising:

search means to search stored filing keys at said remote archive storage means to select at least one of the one or more data blocks for retrieval of copies of the at least one of the one or more data blocks.

26. The system of claim 24, further comprising:

search means to search stored filing keys at said remote archive storage means to select at least one of the one or more data blocks for retrieval of copies of the at least one of the one or more data blocks.

27. The system of claim 2, further comprising:

encryption means for encrypting the one or more data blocks to produce one or more encrypted data blocks such that the remote archive storage means may not decrypt the one or more encrypted data blocks but that the user may decrypt copies of the one or more encrypted data blocks.

28. The system of claim 20, further comprising:

encryption means for encrypting the one or more data blocks to produce one or more encrypted data blocks such that the remote archive storage means may not decrypt the one or more encrypted data blocks but that the user may decrypt copies of the one or more encrypted data blocks.

29. The system of claim 2, further comprising:

voice waveform data input means, coupled to said user data processing means, for receiving a user's voice and creating voice waveform data; and

voice recognition and transcription means, coupled to said user data processing means and said remote archive storage means, for generating one or more text data blocks from said voice waveform data transmission for storage in the remote archive storage means.

30. The system of claim 28, further comprising:

voice waveform data input means, coupled to said user data processing means, for receiving a user's voice and creating voice waveform data; and

voice recognition and transcription means, coupled to said user data processing means and said remote archive storage means, for generating one or more text data blocks from said voice

waveform data transmission for storage in the remote archive storage means.

31. The system of claim 2, further comprising decryption means, coupled to the user data input means and the archive storage means, for decrypting the one or more encrypted data blocks to create one or more decrypted data blocks, and transmitting said one or more decrypted data blocks to the user data processing means.

32. A method for archiving data blocks comprising the steps of:
forming, in a user data input device, one or more data blocks,
transmitting the data blocks from the user using a transmission network,
archiving the one or more data blocks in a remote archive storage, and
preventing anyone, including the user, from modifying or deleting the one or more data blocks stored at the remote archive storage to provide non-rescindable storage of the data blocks for at least an initial time period.

33. The method of claim 32, further comprising the step of negotiating, between the user and the remote archive storage an initial time period to reach agreement on an initial time period for non-rescindable storage of the one or more data blocks.

34. The method of claim 32, further comprising the step of retrieving, from the remote archive storage to the user, a copy of the one or more data blocks.

35. The method of claim 32, further comprising the steps of:
computing, in an encryption data processor coupled to the user data input device, a secure digital signature data block comprising a secure digital signature of the one or more data blocks,
and
appending the digital signature data block to the one or more data blocks.

36. The method of claim 35, wherein the step computing a secure digital signature data block comprises the step of computing the digital signature in a digital signature generating party independent of the user data input device, and coupled to the user data input device via the transmission network.

37. The method of claim 32, further comprising the steps of:
time-stamping in a secure time-stamping device coupled to the user data input device and the remote archive storage, the one or more data blocks upon receipt, and
storing the time-stamp as an additional non-rescindable data block with the one or more data blocks in the remote archive storage.

38. The method of claim 37, wherein the step of time-stamping comprises the step of time-stamping in a secure time-stamping party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage by the transmission network.

39. The method of claim 32, further comprising the steps of:

encrypting, in an encryption device coupled to the user data input device and the remote archive storage, the one or more data blocks to create one or more encrypted data blocks, and

transmitting the one or more encrypted data blocks to remote archive storage in place of the one or more data blocks.

40. The method of claim 39, wherein the step of encrypting comprises the step of encrypting in an encryption party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

41. The method of claim 32, further comprising the step of generating, in a filing key generator coupled to the user data input and the remote archive storage, filing keys from the one or more data blocks.

42. The method of claim 41, wherein the step of generating filing keys comprises the step of generating filing keys in an independent filing key generating party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

43. The method of claim 32, further comprising the step of searching stored filing keys at the remote archive storage to select at least one of the one or more data blocks for retrieval of copies of the at least one of the one or more data blocks.

44. The method of claim 43, wherein the step of searching comprises the step of searching in an independent search party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

45. The method of claim 32, further comprising the step of encrypting, in an encryption device, the one or more data blocks to produce one or more encrypted data blocks such that the remote archive storage may not decrypt the one or more encrypted data blocks but that the user may decrypt copies of the one or more encrypted data blocks.

46. The method of claim 45, wherein the step of encrypting comprises the step of encrypting in an independent encryption party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

47. The method of claim 32, further comprising the steps of:
inputting in a voice waveform data input device coupled to the user data input device, a user's voice and creating voice waveform data, and

transcribing in a voice recognition and transcription device coupled to the user data input device and the remote archive storage, the voice waveform data to create text data blocks from the voice waveform data received from the user data input device for storage in the remote archive storage.

48. The method of claim 47, wherein the step of transcribing the voice waveform data comprises the step of transcribing the voice waveform data in an independent voice recognition and transcription party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

49. The method of claim 33, further comprising the steps of:

computing, in an encryption data processor coupled to the user data input device, a secure digital signature data block comprising a secure digital signature of the one or more data blocks, and

appending the digital signature data block to the one or more data blocks.

50. The method of claim 49, wherein the step computing a secure digital signature data block comprises the step of computing the digital signature in a digital signature generating party independent of the user data input device and coupled to the user data input device via the transmission network.

51. The method of claim 49, further comprising the steps of:

time-stamping in a secure time-stamping device coupled to the user data input device and the remote archive storage, the one or more data blocks upon receipt; and

storing the time-stamp as an additional non-rescindable data block with the one or more data blocks in the remote archive storage.

52. The method of claim 51, wherein the step of time-stamping comprises the step of time-stamping in a secure time-stamping party independent of the user data input device and the remote

archive storage and coupled to the user data input device and the remote archive storage by the transmission network.

53. The method of claim 51, further comprising the steps of:

encrypting, in an encryption device coupled to the user data input device and the remote archive storage, the one or more data blocks to create one or more encrypted data blocks, and

transmitting the one or more encrypted data blocks to remote archive storage in place of the one or more data blocks.

54. The method of claim 53, wherein the step of encrypting comprises the step of encrypting in an encryption party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

55. The method of claim 53, further comprising the step of generating, in a filing key generator coupled to the user data input and the remote archive storage, filing keys from the one or more data blocks.

56. The method of claim 55, wherein the step of generating filing keys comprises the step of generating filing keys in an independent filing key generating party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

57. The method of claim 55, wherein the step of searching comprises the step of searching in an independent search party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

58. The method of claim 47, wherein the step of searching comprises the step of searching in an independent search party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

59. The method of claim 51, further comprising the step of encrypting, in an encryption device, the one or more data blocks to produce one or more encrypted data blocks such that the remote archive storage may not decrypt the one or more encrypted data blocks but that the user may decrypt copies of the one or more encrypted data blocks.

60. The method of claim 59, wherein the step of encrypting comprises the step of encrypting in an independent encryption party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

61. The method of claim 59, further comprising the steps of:
inputting in a voice waveform data input device coupled to the user data input device, a user's voice and creating voice waveform data, and

transcribing in a voice recognition and transcription device coupled to the user data input device and the remote archive storage, the voice waveform data to create text data blocks from the voice waveform data received from the user data input device for storage in the remote archive storage.

62. The method of claim 61, wherein the step of transcribing the voice waveform data comprises the step of transcribing the voice waveform data in an independent voice recognition and transcription party independent of the user data input device and the remote archive storage and coupled to the user data input device and the remote archive storage via the transmission network.

63. A system for decrypting encrypted diary entry data stored over a network, comprising:

archive storage means, for storing one or more encrypted data blocks created by a user, said remote archive storage means preventing anyone, including the user, from modifying or deleting said one or more data blocks stored at said remote archive storage means to provide non-rescindable storage of said data blocks for at least an initial time period;

transmission means, coupled to the user data processing means, for transmitting said data blocks from the user data processing means;

a user data processing means, coupled to the transmission means for a user to retrieve one or more data blocks from the archive means through the transmission means; and

decryption means, coupled to the user data processing means and the archive storage means, for decrypting the one or more encrypted data blocks to create one or more decrypted data blocks, and transmitting said one or more decrypted data blocks to the user data processing means.

64. The system of claim 63, wherein the decryption means comprises an decryption party, independent of the user data processing means and the remote archive storage means, coupled to the user data processing means and the remote archive storage means via the transmission means.

65. The system of claim 63, further comprising decryption keys for said decryption means, said keys being non-rescindably stored in a non-rescindable key store.

66. The decryption system of claim 65, further comprising user assured access to said decryption keys in said non-rescindable store.

67. The decryption system of claim 66, further comprising a means for requiring verified personal data of the user by said non-rescindable store in order for said user to have assured access to the decryption keys.

68. The decryption system of claim 65, wherein said non-rescindable store comprises an independent decryption key non-rescindable archive party.

69. The system of claim 3, said archive providing assured access to said means for retrieving data.

70. The system of claim 69, wherein said archive requires verified personal data from said user for providing said assured access.